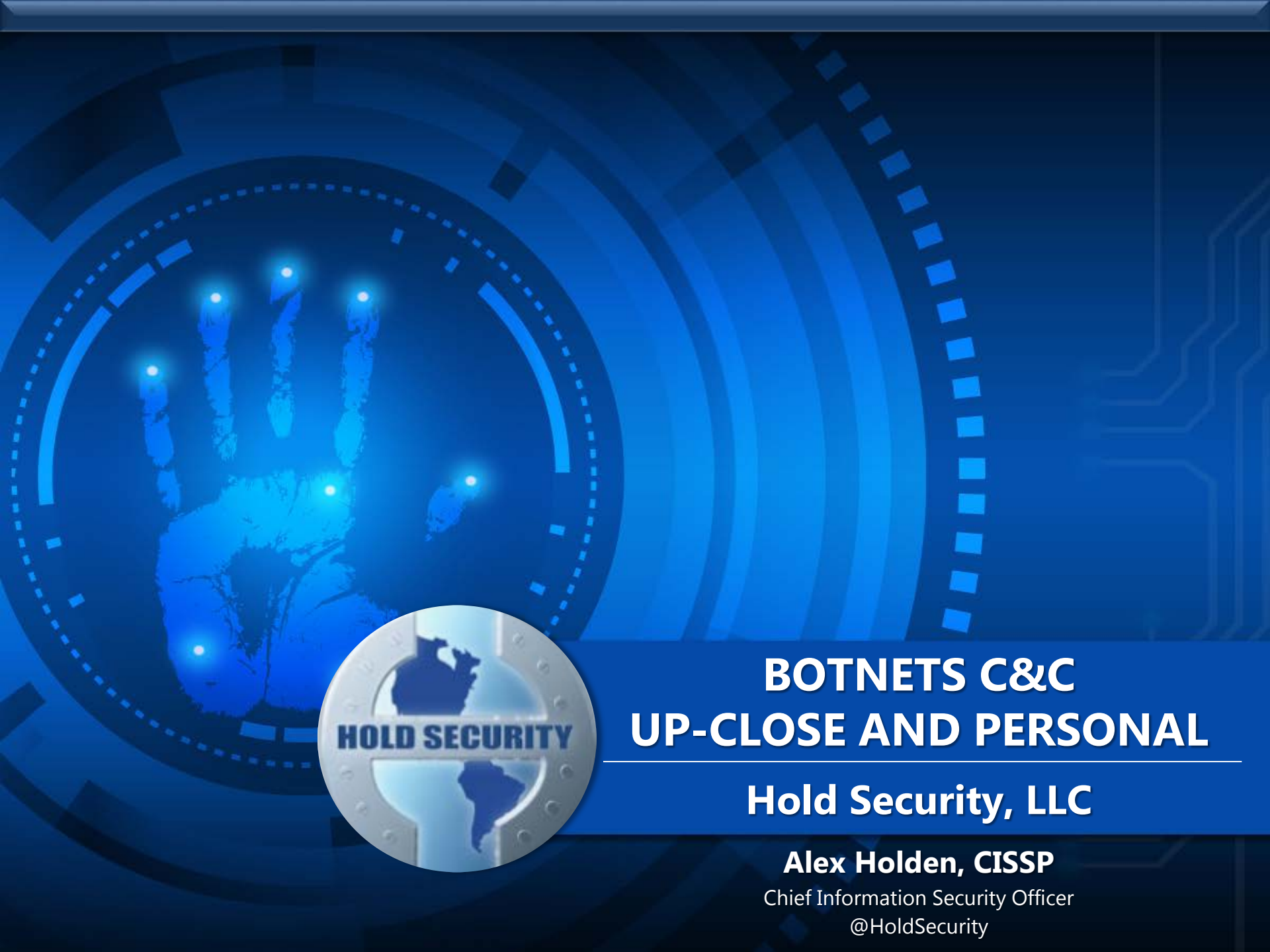


BOTNETS C&C UP-CLOSE AND PERSONAL

Hold Security, LLC

Alex Holden, CISSP
Chief Information Security Officer
@HoldSecurity

WHO AM I AND WHY AM I HERE?

Hold Security Threat Intelligence Program

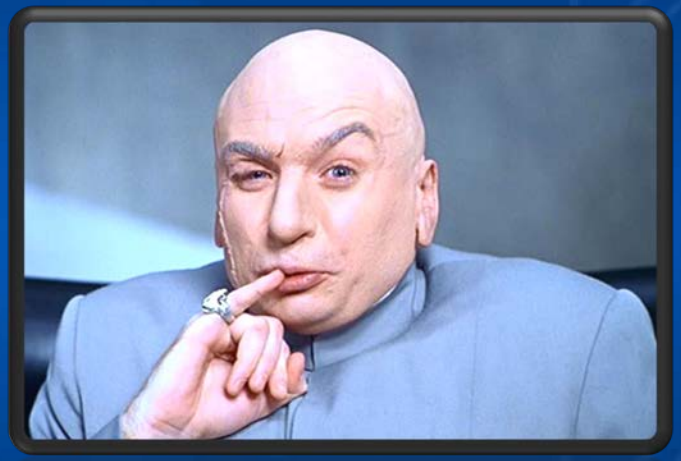
- 2,500,000,000 stolen credentials recovered
- 2,000,000 site breaches identified
- 50,000,000 stolen financial records retrieved
- Thousands of breaches prevented

- Adobe System Breach 2013
- Target Brands Breach 2013
- JP Morgan Chase breach 2014
- Insights into 60% of major security breaches since 2009

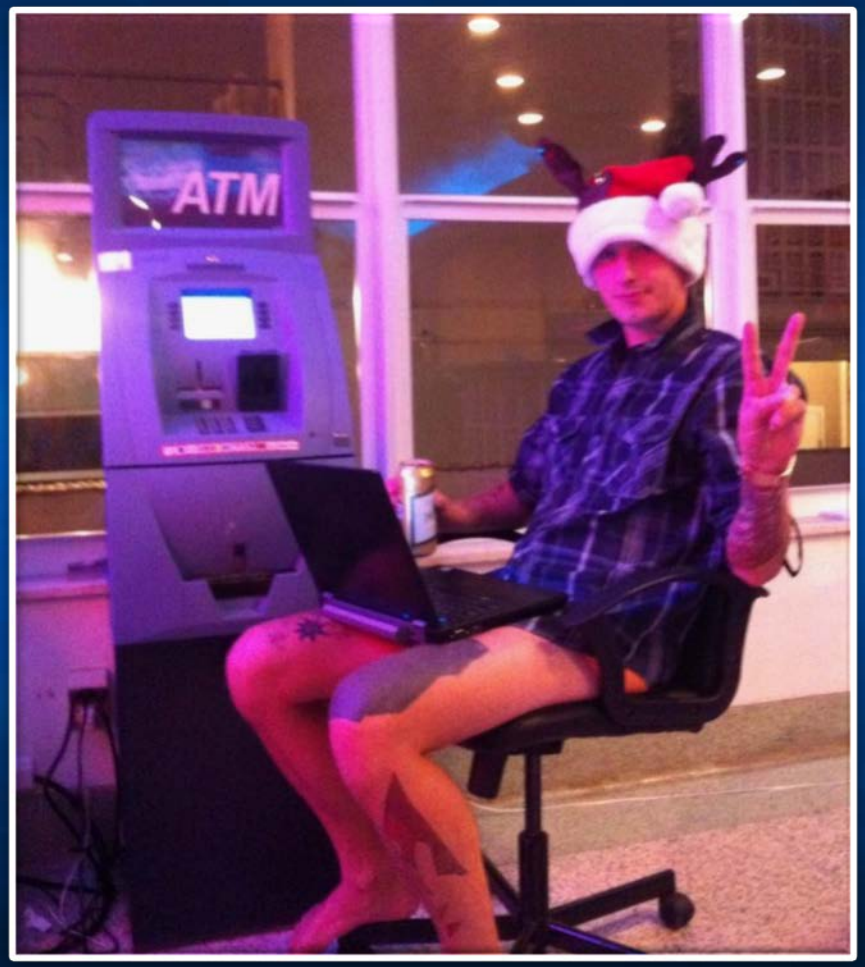
ABOUT ME

- 10 years CISO in a major brokerage firm
- Security researcher and bug hunter
- Pen tester and auditor
- Hacker Hunter

WHO IS THE MODERN HACKER?



MODERN HACKER



MODERN HACKER

HACKERS VIEW OF US

- **War of stereotypes**

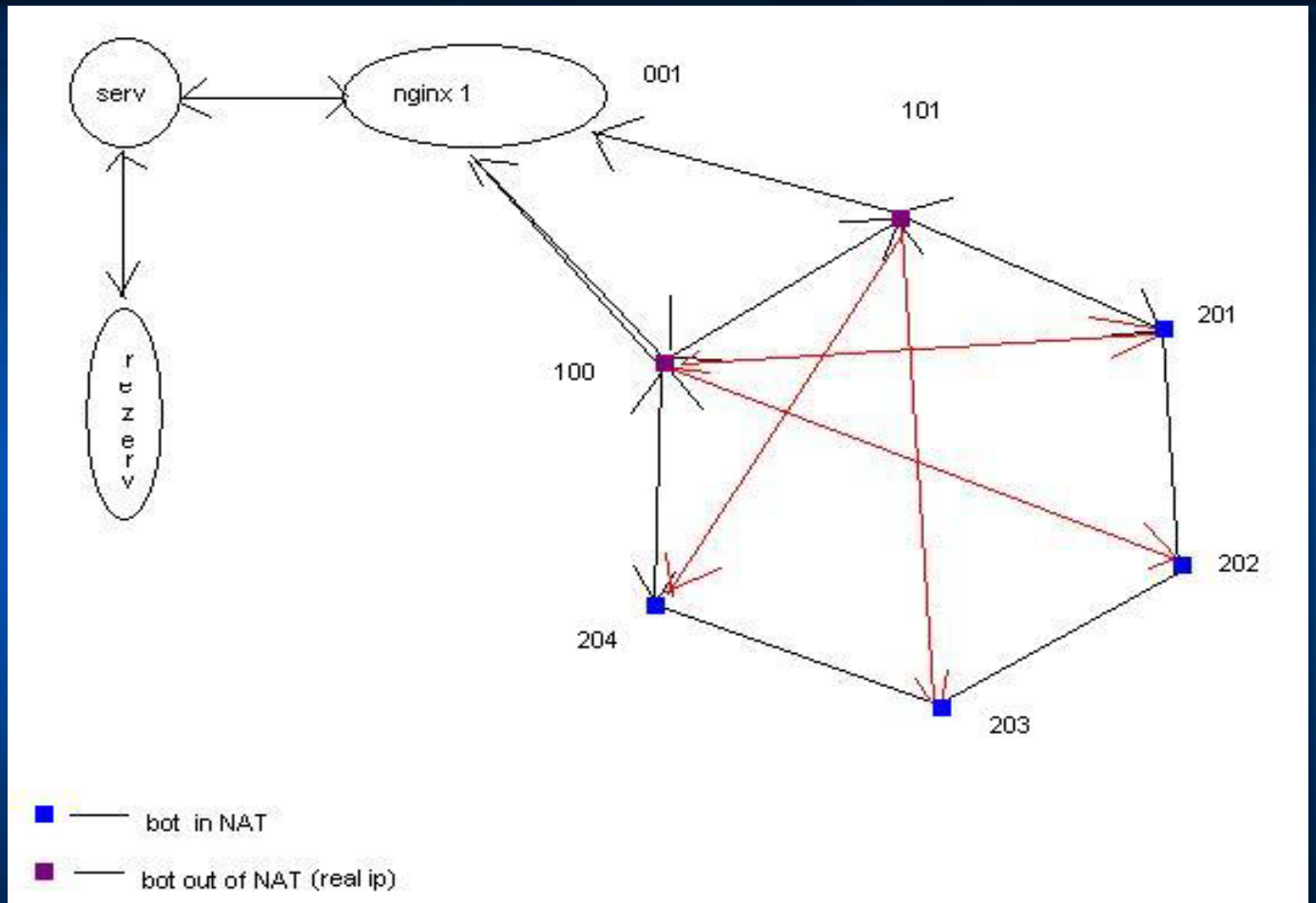
"I'm fighting a holy war against the West... They drive their Rolls Royces and go home to their million-dollar houses, while people here are struggling. I will never harm my fellow Slavs; but America, Europe, and Australia deserve it."

- aqua (jabberzeus)

BOTNET LIFE-CYCLE

FROM BLACKMAIL TO BLACKMAIL

BOTNETS - NEW LEVEL OF SOPHISTICATION



на 10х создаются промежуточные серве для сливания
на главный серве, список меняется каждые 10 - 20 минут
101 и 100 переодически сливают на главны или другу
другу, в то время 20х сливают все только на 10х и
также перодично на разные 10х чтоб путать цепочку.
Список ип обновляется с радомным порядком

SO YOU DECIDED TO BUILD A BOTNET

Step 1:

Rent Exploit Kit

Step 2:

Rent or Build Botnet C&C

Step 3:

Crypt (obfuscate) Payload

Step 4:

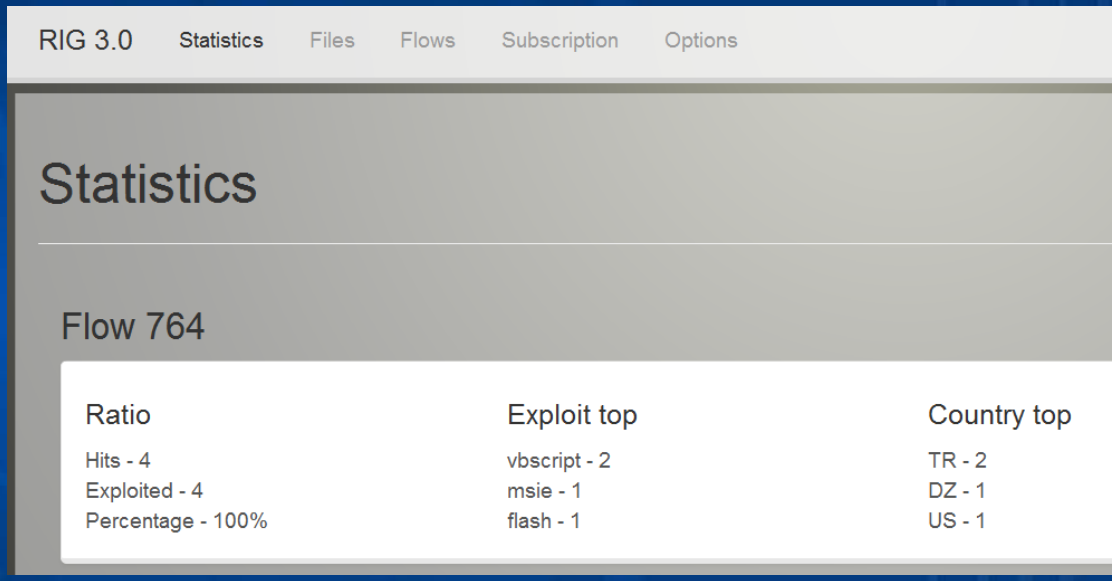
Rent a Virus Distribution Network

Step 5:

Configure and Start Collecting Data

EXPLOIT KITS 101

- Popular
  - Windows
  - MS Office
  - Flash
  - Java
- Not always 0day
- Easy rent by day or week



What about Anti Virus?

Stats | Bots | Scripts | Reports | DGA | Updater | Config | Logout

Current version: 1.4.1
GMT: May 19 2016 15:36:29

Bots	Online	Online per week	Online per 24 hour	Dead bots	Installs per week	Installs per 24 hour
1626	247 (15.2%)	478 (29.4%)	361 (22.2%)	1063 (65.4%)	32	4

Windows	X32	X64	
XP	103 (6.3%)	0 (0.0%)	103 (6.3%)
Vista	4 (0.2%)	0 (0.0%)	4 (0.2%)
Server 2008	12 (0.7%)	67 (4.1%)	79 (4.9%)
Seven	263 (16.2%)	693 (42.6%)	956 (58.8%)
Server 2008 R2	0 (0.0%)	232 (14.3%)	232 (14.3%)
Eight	0 (0.0%)	3 (0.2%)	3 (0.2%)
Server 2012	0 (0.0%)	27 (1.7%)	27 (1.7%)
Eight+	1 (0.1%)	73 (4.5%)	74 (4.6%)
Server 2012 R2	0 (0.0%)	82 (5.0%)	82 (5.0%)
Ten	9 (0.6%)	57 (3.5%)	66 (4.1%)
	392 (24.1%)	1234 (75.9%)	

Antivirus	All	Online
Unknown	1074 (66.1%)	204
TrendMicro	229 (14.1%)	23
MSE	112 (6.9%)	10
McAfee	87 (5.4%)	3
Avg	36 (2.2%)	1
KIS	32 (2.0%)	4
Nod32	29 (1.8%)	2
Avira	19 (1.2%)	0
Avast	8 (0.5%)	0

(This screenshot has been altered for viewing purposes)

OBFUSCATION (CRYPTING)

BOT SHOP

Balance: 3.95$

- News
- Settings
- Balance
- Tasks
- FAQ
- Price list

Add Task | Update

#	URL	Country	Achieved	Limit	Status	
1	http://ch34427.tmweb.ru/dfu7ZrvYQw.exe	Brazil	4	1250	Removed	-
2	http://ch34427.tmweb.ru/BaoywGGnxh.exe	Europe	116	1000	Removed	-
3	http://ch34427.tmweb.ru/lU8qROgvKU.exe	China	0	1000	Removed	-
4	http://ch34427.tmweb.ru/WVMQMYltxQ.exe	China	0	1000	Removed	-
5	http://ch34427.tmweb.ru/WVMQMYltxQ.exe	Brazil	0	1000	Removed	-
6	http://ch34427.tmweb.ru/mN1kykndvi.exe	China	0	1000	Removed	-
7	http://ch34427.tmweb.ru/mN1kykndvi.exe	Brazil	1	1000	Removed	-
8	http://ch34427.tmweb.ru/mN1kykndvi.exe	Brazil	3	1000	Removed	-
9	http://ch34427.tmweb.ru/mN1kykndvi.exe	Turkey	10	1000	Removed	-
10	http://ch34427.tmweb.ru/dtoAq9gIK8.exe	Brazil	0	1000	Removed	-
11	http://ch34427.tmweb.ru/mN1kykndvi.exe	Uzbekistan	27	1000	Removed	-
12	http://nynewsguardianinternet.com/oreon/msdoc.exe	Ukraine	2	1650	Removed	-
13	http://nynewsguardianinternet.com/oreon/55z/doc.exe	Ukraine	4	1000	Removed	-
14	http://nynewsguardianinternet.com/oreon/55z/doc.exe	Ukraine	1	1000	Removed	-

WHAT I NEED TO KNOW ABOUT BUILDING C&C?

[the rest of this slide is intentionally left blank]

Toolkits

- Botnets
- Bots
- Crackers
- Crypters
- Denial of Service
- Forensic Tools
- Icons
- IP & Port Scanners
- Keyloggers
- Misc
- Misc. Ebooks
- Misc. Web Tools
- Network Tools
- Proxy Grabbers
- Rats
- Resolvers
- Shells
- SMS & Email Bombers
- Source Codes & Scripts
- VPNs & Security Tools
- Worms, Malware, & Virus Makers

- µBot
- Aldi v2
- Andromeda v2.06
- Ann Loader
- AnnLoader
- Brainbot
- Cythosia
- DirtJumper V3
- Elite Loader 3.0
- HerpesNet
- Kbot Builder
- Pandora
- Pony 1.9
- SmokeBot Cracked
- Strike
- umbra
- Umbra Loader
- VertexNet
- VertexNetv1.2.1
- vnLoader
- vOlk 4
- Warbot
- YZF
- Zemra

- adf.ly AdfBotPro [3.3.1]
- Aspire Multiuser Account Maker
- Auto Clicker
- GSearchBot3.2.5-rev3
- LambaTube
- mpgh.net Spammer
- msn freezer
- Skype spammer
- Snapchat Bomber
- Tiger Bot Cracked by IoY
- Tubenoia
- Ultimate Codename Likes [Cracked Gold Edition]
- Youtube Blazzer [V1.0]
- Youtube View Booster V1.2
- Youtube View Booster Ver. 1.2, Cracked- PRO EDITION!
- YouView_bot_v1.2
- ZeroTeam Email Spammer v2.1.0.0
- Anonymous JCC Autoclicker
- Auto Clicker
- BTI Pastebin Mass Downloader
- Chrome Skype Spammer
- Cranksy's IceAge
- DeLuXe Chat Spam
- EliteOP - Youtube Tool
- Eternals Auto Typer
- Insatiable 2

- InstaGet v1.2.7 Free
- Instagram Bot
- iSub4Sub - Version 1.1
- iVeiw_For_you
- Jays_youtube_bot_v1.0b
- LikeaPros SkypeCrasher
- Minecraft IN-Game ChatSpammer V1.0 By KWHful
- NET BOT
- Normal In-Chat ChatSpammer V1.0 By KWHful
- Nuisance Pack
- OmegleSpyX v1.8a
- OmegleSpyX v3.2
- Random Username Generator v1
- Republic Hax SpamGen
- Sharecash Survey Helper
- SkypeCrasher
- Snowstone_Cracked
- System32DK YouTube W
- Type_Click
- Universal Chat Spammer
- VBSpam
- Vulcan Handy Spammer
- YouBoosterPRO Cracked By Heat
- Youtube_view_increaser

- BatchNΣT + OpenSource
- bRAT + source_code
- [SRC] BIODOX
- [SRC] Zombie Slayer
- AndroRAT
- Babylon 1.6.0.0
- BatchNΣT
- Beast 2.06
- Bifrost 1.2.1d
- Blackshades Public Edition
- Blizzard 1.2
- BlueBanana
- Cybergate 1.8
- Dark Comet 4.0
- Dark Comet 5.1
- Dark Comet 5.3
- DarkMoon 4.11
- DroidJack 3.0
- DroidJack 4.0
- Gklspy
- ip killer
- jRat
- jSpy
- KazyBot 1.0 Lite
- Loki Rat
- Lost Door 2.2 Public
- MiniMo 0.7a Public Lite
- NjRAT 0.7
- NovaLite v3.0
- Nuclear RAT 2.1.0
- Optix 1.33
- Paradox RAT
- Poison Ivy 1.0
- Poison Ivy 2.3.2
- Quasar 1.1
- SharK 3.0
- Spycronic 1.02.1
- SpyNet 0.7 Public
- Spy-Net v2.6
- Sub-7 0.10
- Tiny 0.2
- Turkojan 4.0 Gold
- xRAT 2.0
- XtremeRat 3.5

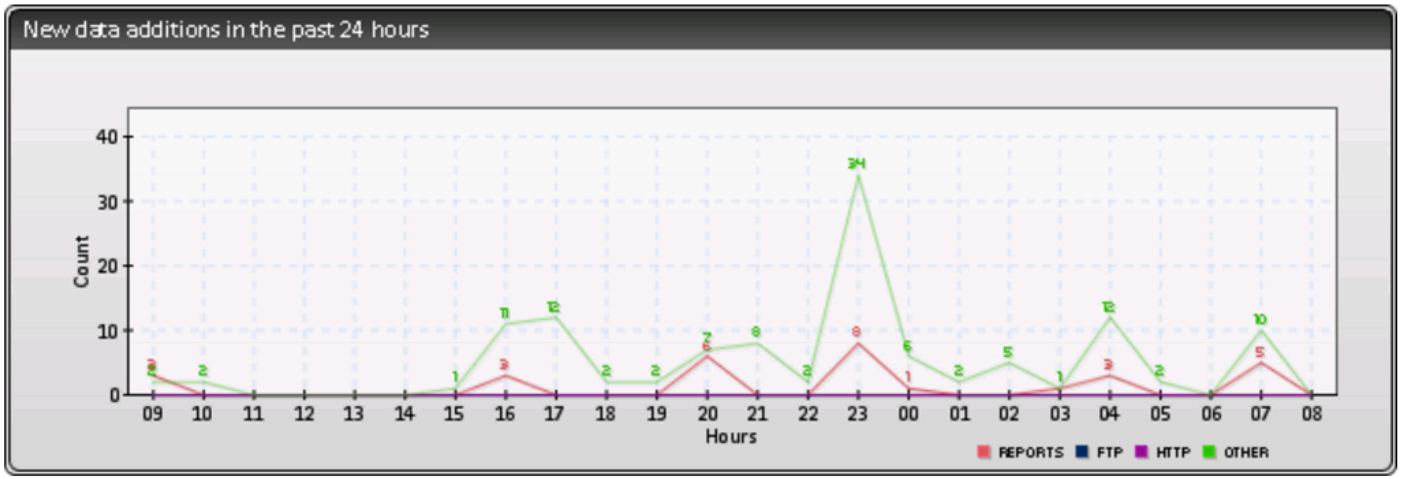
BUILD YOUR OWN DISTRIBUTION NETWORK

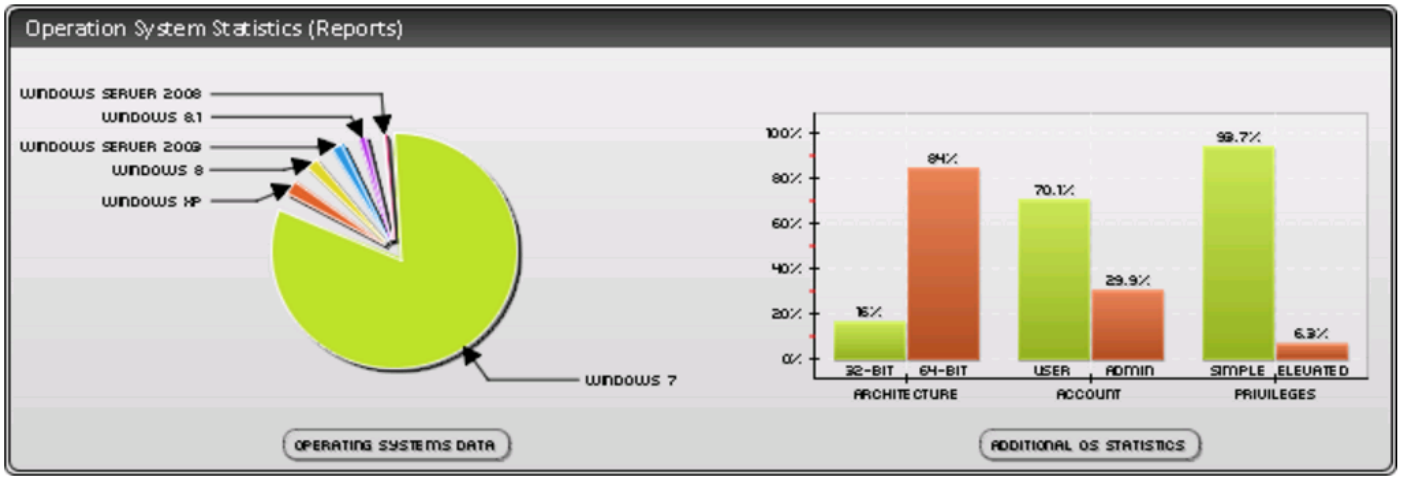
- Traffic Traffic Traffic
- Look at the statistics

BOTNET DEMO

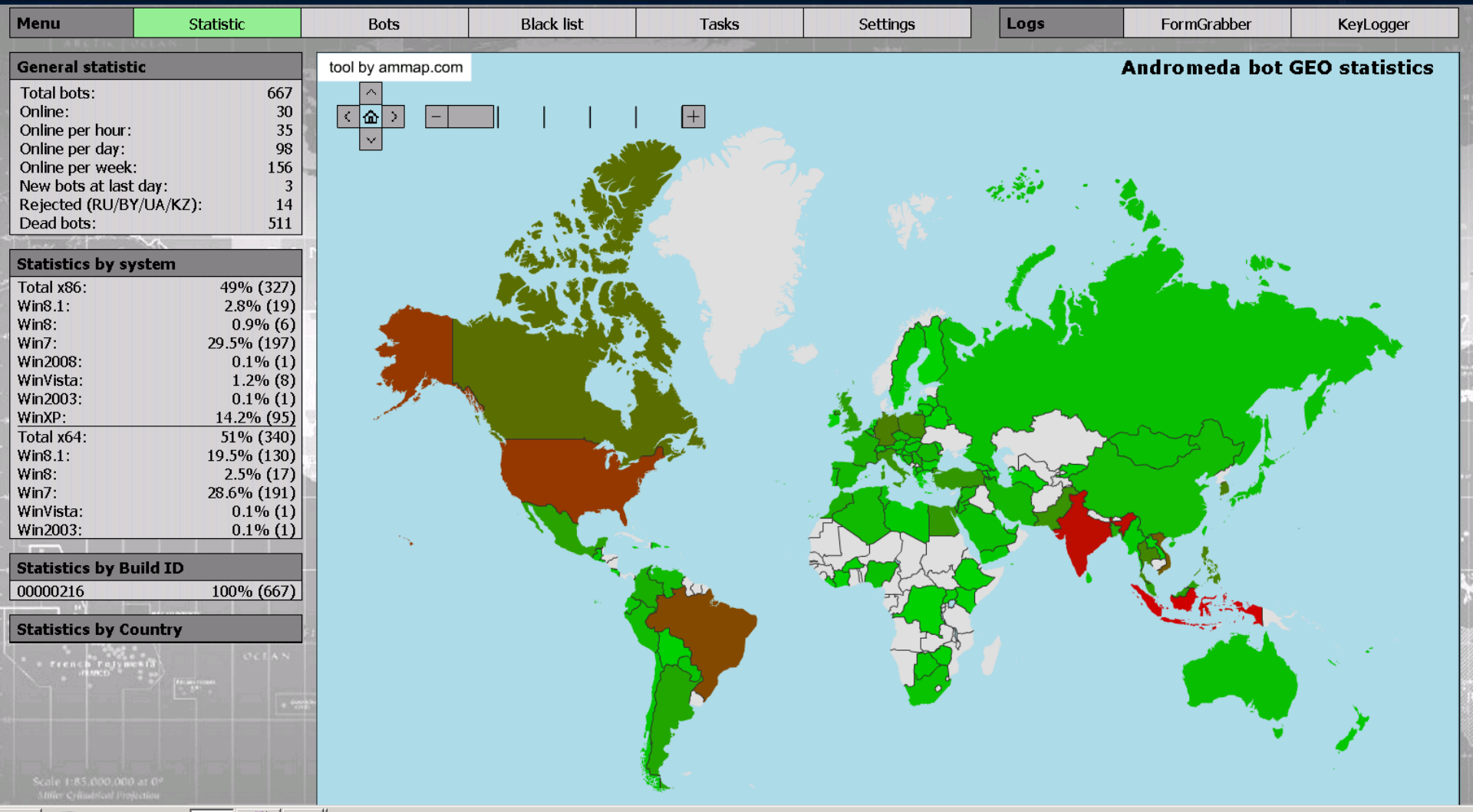
LOKI

Loki PWS | Main | HTTP | FTP/SSH | Others | Reports | Settings | Exit

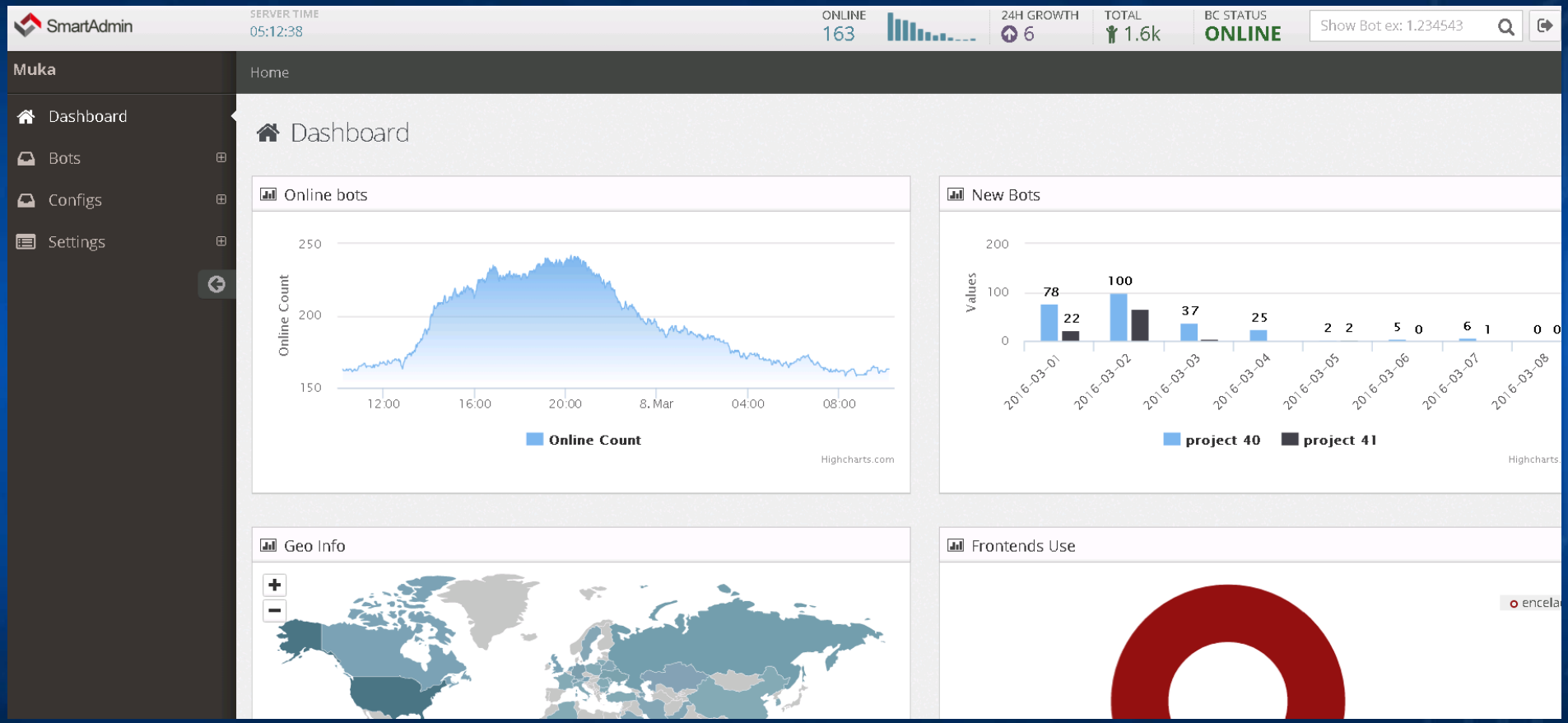




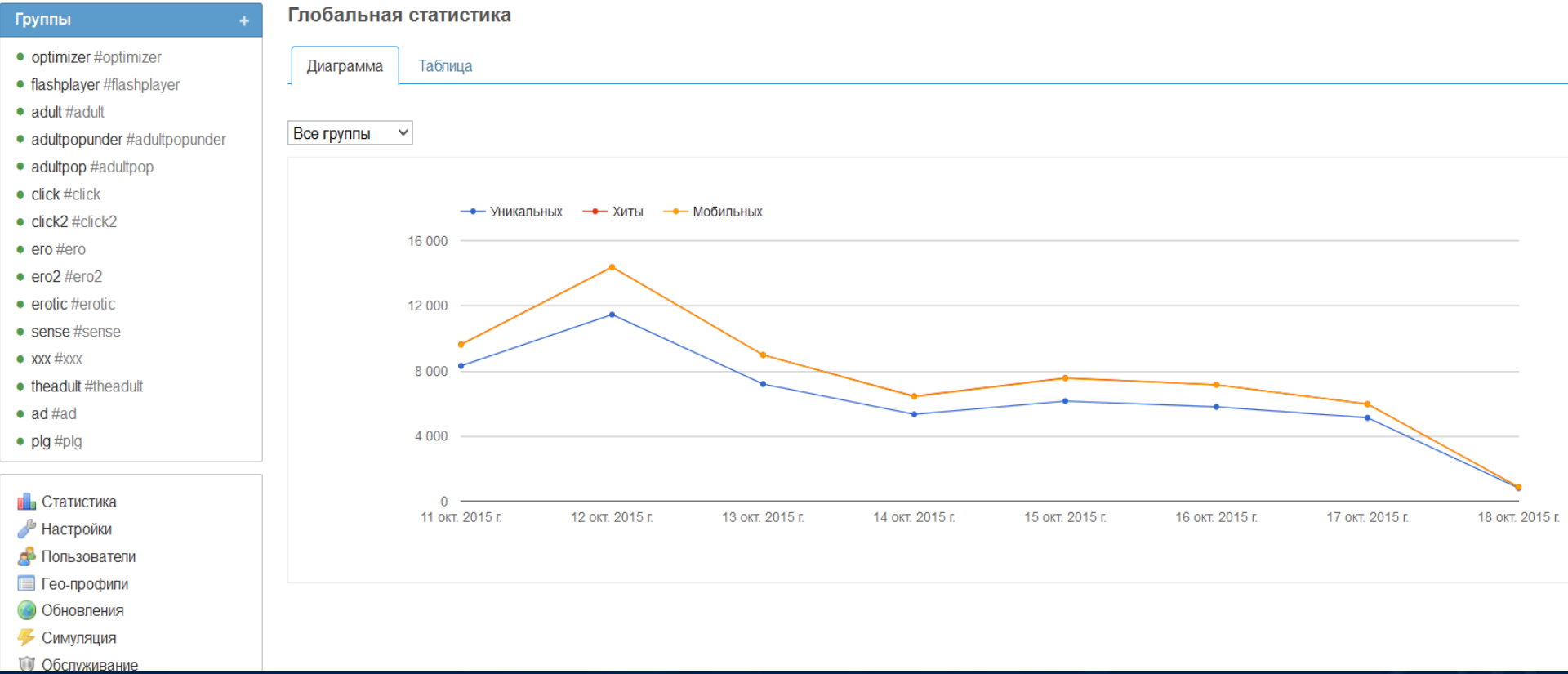
ANDROMEDA


Menu
Statistic
Bots
Black list
Tasks
Settings
Logs
FormGrabber
KeyLogger
General statistic
Total bots: 667
Online: 30
Online per hour: 35
Online per day: 98
Online per week: 156
New bots at last day: 3
Rejected (RU/BY/UA/KZ): 14
Dead bots: 511
Statistics by system
Total x86: 49% (327)
Win8.1: 2.8% (19)
Win8: 0.9% (6)
Win7: 29.5% (197)
Win2008: 0.1% (1)
WinVista: 1.2% (8)
Win2003: 0.1% (1)
WinXP: 14.2% (95)
Total x64: 51% (340)
Win8.1: 19.5% (130)
Win8: 2.5% (17)
Win7: 28.6% (191)
WinVista: 0.1% (1)
Win2003: 0.1% (1)
Statistics by Build ID
00000216 100% (667)
Statistics by Country
tool by ammap.com
Andromeda bot GEO statistics

ONYX / DiamondFox



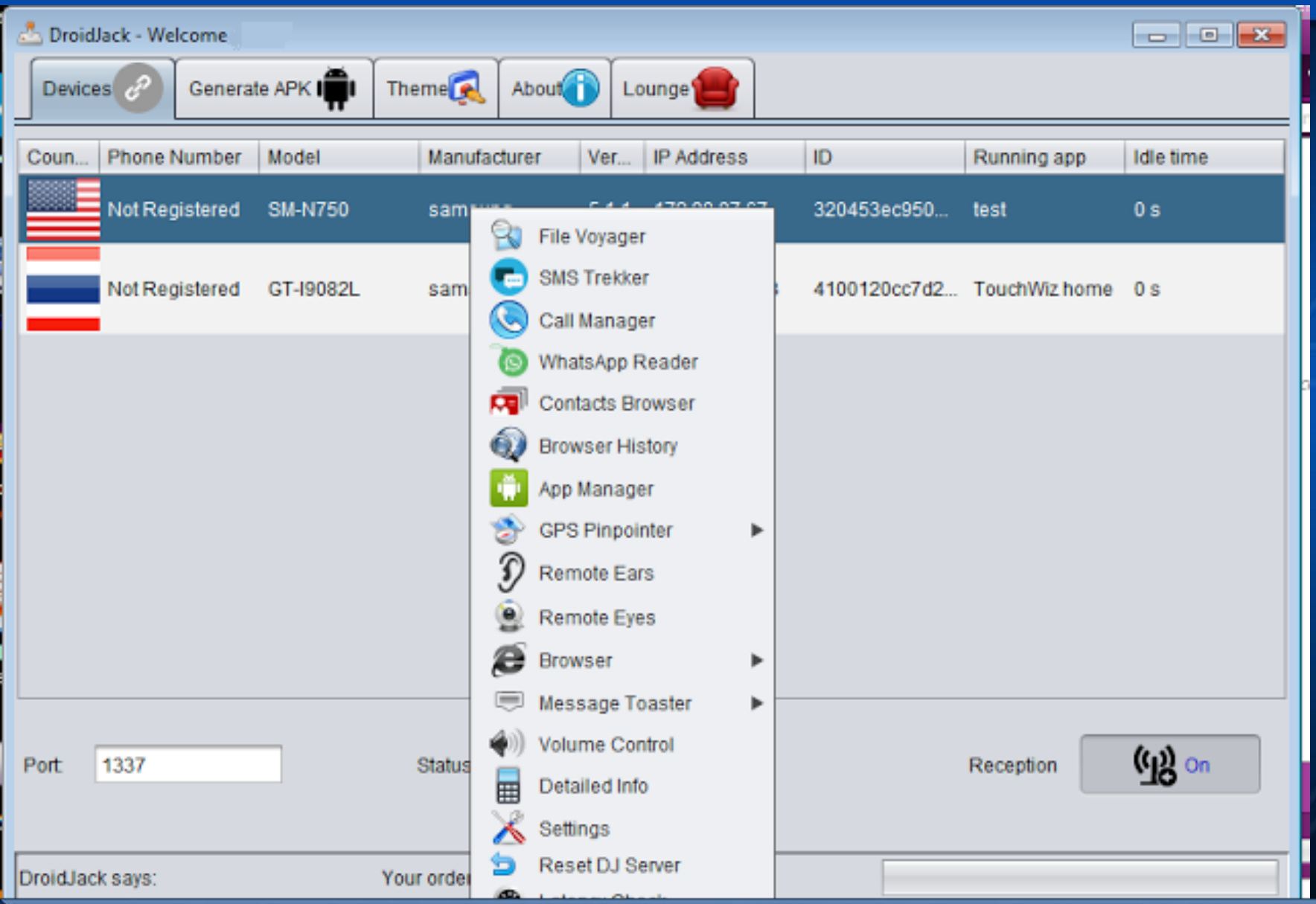
MOBILE BOTNETS



Injects and Grabbers

- User experience hijacking
- Specific data accumulation

RATs


DroidJack - Welcome
Devices
Generate APK
Theme
About
Lounge
Coun...
Phone Number
Model
Manufacturer
Ver...
IP Address
ID
Running app
Idle time
Not Registered
SM-N750
320453ec950...
test
0 s
Not Registered
GT-I9082L
4100120cc7d2...
TouchWiz home
0 s
File Voyager
SMS Trekker
Call Manager
WhatsApp Reader
Contacts Browser
Browser History
App Manager
GPS Pinpointer
Remote Ears
Remote Eyes
Browser
Message Toaster
Volume Control
Detailed Info
Settings
Reset DJ Server
Port:
1337
Status
Reception
On
DroidJack says:

DEFENSE - HONEYPOTS

Honeypots are not only systems

- Components
- Credentials
- Features

CONCLUSIONS

- Botnets are BAD
- Clever and Complicated
- Botnet collect everything
- Can stop them

THANK YOU

Hold Security, LLC

Alex Holden - aholden@HoldSecurity.com